CEO CFO

e-sentire™

Issue:
June 3, 2013

All rights reserved!
ceocfointerviews.com

CEOCFO Magazine - The Most Powerful Name In Corporate News and Information

As the 24/7 Electronic Security Guard for their Customers, eSentire has reinvented Enterprise Network Security by focusing on a Human Driven, Behavior-Based Solution that Defends Against the New Generation of Threats

Technology
Managed Security Services

eSentire
278 Pinebush Road, Suite 200
Cambridge, ON N1T 1Z6
519.651.2200 / 866.579.2200
www.esentire.com

J.Paul Haynes
CEO

BIO:
Mr. Haynes joined the firm in 2010 to bring his expertise in sales, marketing and growth strategies to the organization. He has started, financed and sold a number of enterprise software businesses in sectors including energy, government, healthcare and engineering and technologies including ERP, CRM, ECM, CIS and Project Management. Mr. Haynes is a professional engineer and holds a Masters in Engineering and sits on several Boards of Directors.

About eSentire:
eSentire has reinvented enterprise network security by focusing on protecting your core assets inside the network through our human driven, behavior-based solution. We turn the traditional layered security approach on its ear as we assume your network is already compromised. We detect behaviors indicative of advanced threats from criminals, nation states or activists and even your own staff whether malicious or borne of ignorance. No matter where you are we have your back 24x7x365.

Interview conducted by:
Lynn Fosse, Senior Editor
CEOCFO Magazine

CEOCFO: Mr. Haynes, what attracted you to eSentire?
Mr. Haynes: When considering joining eSentire as CEO, I had already been with a number of firms and vertical markets. This time I decided to do a little bit of diligence on the customer base and met many of them at an event in NYC. Among other things that attracted me to the firm was something I had never seen before which was such fanatically enthusiastic customers. We went to two marketing events and at each there were three or four customers in attendance and fifteen or twenty prospects. I sat back and watched the sales guy let the customers sell the company to the prospects. I have never seen anything like it before. The other one is that the company's business model is based on a partnership with the customers to deliver a day-in-day-out 24/7 essential service. Because of that, you end up with a very predictable revenue stream and business model. Therefore, it makes planning the business much easier and not as lumpy as the traditional enterprise software.

CEOCFO: Your tagline is Get Protected Stay Safe. How do you make that happen?
Mr. Haynes: Our core value in the company is "we always have our customers back." The customers come to depend on us to monitor their network to protect against advanced threats which come in many forms and include intrusion and data extractions, theft of confidential corporate information, illicit funds transfer, defacing of websites and what they call denial of service attacks. Our job is to be that 24/7 electronic security guard for our customers. We protect the networks and we have capabilities very specific to defend against the new generation of threats.

CEOCFO: Yours is a crowded field certainly and everyone will tell you they have the best and the latest as well as the greatest. What is the approach at eSentire and how does it differ from the others? What do you know that is better, faster cheaper as well as easier and more effective?
Mr. Haynes: I am not convinced that we are cheaper but I am convinced that we are categorically much more effective. The perspective that we take is quite different than the rest of security. The security industry has evolved around building better security fences and it is all around protecting from a perimeter perspective and being able to identify an already seen threat that you see coming from the outside and preventing it from coming

in. It started with firewalls and anti-virus and it has evolved to intrusion detection, application firewalls and so on. We take a completely different perspective which is we are looking from the inside of your network for abnormal behaviors and other activities that are indicative of your network already being compromised. It is a very different problem to solve and it is based on advanced detection. Perimeter based security approaches work very effectively at blocking a threat that has already been seen. The way it typically works is the malware is captured and quarantined. From there you learn the unique mathematical formula that describes its DNA and then you write an algorithm to block any time that mathematical formula presents itself. In our world of advanced threats, we have to block against something that has never been seen before so you cannot use this mathematical formula approach. What you have to do is look for some mathematical matches and marry that up with abnormal behaviors such as surges of data flowing through user workstations, use of encryption techniques that have never been seen before, connections to internet locations that are outside of the company's policy like China or Russia for example where threat actors are known to be, and any or all of these things happening at 2:00 am. What you have to do is correlate all of those behaviors together along with whatever mathematical evidence you have and make the call that this is an atypical activity and then intervene. The way we intervene is use of our forensic capture system. We log all of the data flowing on the customer's network and can replay what happened to anybody's workstation and trace the before and after state. In our world forensic means three minutes ago and not three months or three years ago. This data is critical to determine if they have been attacked and if we see that they have been attached we put active blocks in place.

CEOCFO: When you evaluate a new project do you go back six months to have a baseline?

Mr. Haynes: One of the main challenges that most organizations lack full forensic capture and the ability to do real-time intervention. While large banks, defense contractors and other similar scale organizations have forensic capabilities and some intervention capabilities, this is generally cost prohibitive for most firms – that is before eSentire came along. When we are engaged to conduct a security review with new customers – our Get Protected offering in our tagline - we generally have very little historical electronic evidence available for us to work with. We start by implementing our forensic capture and monitoring capability and let it run for 30 or 45 days. This gives us an excellent starting point of what your current security posture is as we see EVERYTHING that flows on your network. The term "you don't know what you don't know" could never be more true the first time a customer sees what is actually happening on their network. When you compare actual network activity to what is allowed based on the acceptable use policy, CFOs and Risk Officers are left typically in state of disbelief. Without a tool like ours, you cannot monitor the compliance with policy. In fact once using our continuous monitoring service, over 2/3 of our customers never let the system leave their network. In doing a security review we tend to focus on the traffic that somehow passes through the firewall and what damage it can do on the inside – the so called inner attack surface. The firewall represents the external attack surface. To contrast them, the inner attack surface is often 30X greater than the external attack surface and also is usually where the "secret sauce" is located. To assess your susceptibility to attack, we also look at workstations and look to see if they have the most current software updates applied. If they do not, that increases their vulnerability as it makes it that much easier for the bad guys. We do this so often that we have developed a very standardized process. It is not uncommon during a security review to find something that is in the high or critical stage such that we have to halt our work and identify it to the customer so they can remediate immediately. For the customer considering doing this on their own, they would have to buy tools that would cost more than $100 thousand dollars which is considered to be too much and too expensive and require skills that are too specialized. The way eSentire does this is make it easy for the customer and actually include the sensor as part of our security review. Just a couple weeks ago we found a customer that was under active attack trying to establish a connection to an Asian-based command and control center where the threat actors were attempting to start extracting customer data they found on the network. We caught it and stopped it right in the middle of the process. While these attacks may only happen to your firm once every ten or twenty months, they do happen and if you aren't looking for it you will never know it occurred.

"When you compare actual network activity to what is allowed based on the acceptable use policy, CFOs and Risk Officers are left typically in state of disbelief."- J.Paul Haynes

CEOCFO: Do you find that most firms today understand the need to protect from the inside out or is that still a learning curve for most?

Mr. Haynes: To a certain extent, the Wall Street Journal and New York Times recently brought a lot of attention to this type of attack. Not to pick on them but what they have done is a great deal of awareness building for the type of attack that we are especially good at protecting against. There are other older examples such as Google, Oak Ridges Lab and RSA, which is a big security company who was believed to be attacked in order to break into a defense contractor. What we often use to educate the prospective customer is "if you do not want this to happen to you" then you need to look at a solution like ours. Once you explain to a prospective customer how these advanced attacks work, it is quite fascinating to see them realize how easy they have made it for threat actors to break into their network. When you describe how they are basically susceptible to opening an email that has been infected, and the way that the threat actors target individuals through what is called social engineering, it is scary. Social engineering is the term used to describe how threat actors, using for example your Facebook profile, can fake an email identity and apply enough context so that it looks real enough and perhaps from one of your colleagues that you open it or the file that is attached and it is over, you have been compromised and you won't even know it. Who would not open a document about a salary survey amongst your peers from someone you know. The PDF or Excel file that you open has something hidden inside of it we call the payload and from the point that this gets on your machine onward you are compromised and you will never know that anything has happened. From here, the threat actors via remote control instructions effectively pretend that they are you on the network and can then create connections to external locations on the internet and instruct the advanced malware so they can roam your network and steal the information they are seeking. Over the course of days or weeks, the threat actors find out your passwords and then move laterally within your network and for example look for treasury functions where they can steal wire transfer instructions and literally conduct wire transfers to their accounts. We make it that easy for them.

CEOCFO: How has eSentire changed under your leadership and what do you see ahead for the company?

Mr. Haynes: When I joined the company, the two founders that recruited me were self-described as technical nerds – very good ones I might add. They were looking to bring someone in who would change the company from a technology building firm to a sales and marketing driven organization. I came into the business and studied the metrics, operating parameters, market prices and developed a business plan which I was able to put in front of equity investors and secured a series of venture capital rounds. That provided enough firepower to expand our development and sales organizations as well as build the leadership team. Our primary market is alternate investment managers and our emerging markets are IP driven organizations and data centers. In that two-year period we have tripled our customer base for direct customers and established a channel who have added another few hundred customers who we secure on the partner's behalf. We have also managed to secure beachhead accounts in all the new sectors that we have targeted.

CEOCFO: How are you reaching your potential customers?

Mr. Haynes: We are in a world of the customers finding the supplier now versus the other way around, so you cannot hope to have a chance in this new world without having a very significant web presence. To make this work we employ extensive search engine optimization so you make it easy for the customers to find you. There is another activity around thought leadership where our advanced threat experts need to put white papers out and do webinars. We have created a highly efficient web marketing machine.

CEOCFO: Why should the business and investment community pay attention to eSentire? Why is eSentire an exceptional company?

Mr. Haynes: What makes eSentire exceptional is we have a unique way of making the information security problem go away including this next generation of advanced threats. Why it is particularly relevant to finance is that this is one of the better educated sectors where executives understand risk management. We operate in markets where there is a high sensitivity to the risk associated with a security breach such as public relations, investor risk and regulatory risk. We help substantially reduce that risk and have a proven very high efficacy in terms of minimizing financial and data loss. The other attribute about the organizations we are typically dealing with, is that their main business is stock trading, executing orders and market strategies – but what it is not is information security. They have extremely high exposure to information security risk and we are the trusting partner that makes it go away. We make the problem go away, we have rapid set up and we deliver a service that is 24/7.

eSentire

**278 Pinebush Road, Suite 200
Cambridge, ON N1T 1Z6
519.651.2200 / 866.579.2200
www.esentire.com**